



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/669,784	09/24/2003	James C. Farmer	10002762-3	6401

7590 01/04/2007
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

TSAI, SHENG JEN

ART UNIT	PAPER NUMBER
----------	--------------

2186

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/669,784

Applicant(s)

FARMER ET AL.

Examiner

Sheng-Jen Tsai

Art Unit

2186

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 September 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 September 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>09/24/2003</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-20 are presented for examination in this application (10,669,784) filed on September 24, 2003.

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 1-20 are rejected under the judicially created doctrine of anticipation-type double patenting as being anticipated by claims 1-16 of US Patent **6,658,543** (Farmer et al., "System and Method to Protect Vital Memory Space from Non-malicious Writes in a

Art Unit: 2186

Multi Domain system"), as shown in the following table. Although not all of the conflicting claims are exactly identical, they are extremely similar and are not patentably distinct from each other as shown below:

10/669,7845	6,658,543
1. A method for protecting memory space in a target storage device during a write operation in a computer system, the method comprising: creating a single data packet, including user data that is to be written to said target storage device and key data that is used to establish authorization to store said user data; transmitting said single data packet to the target storage device; determining whether said key data is valid; writing said user data into said target storage device only when said key data is, valid.	1. A method for protecting memory space in a target storage device during a write operation in a computer system, the method comprising: creating a single data packet, including user data that is to be written to said target storage device and key data that is used to establish authorization to store said user data; calculating key data based on gathered user data; combining said gathered user data and said calculated key data to form said composed single data packet; transmitting said single data packet to the target storage device; determining whether said key data is valid; writing said user data into said target storage device only when said key data is valid.
2. The method of claim 1 further comprising: calculating key data based on said gathered user data; and combining said gathered user data and said calculated key data to form said composed single data packet.	1. A method for protecting memory space in a target storage device during a write operation in a computer system, the method comprising: creating a single data packet, including user data that is to be written to said target storage device and key data that is used to establish authorization to store said user data; <u>calculating key data based on gathered user data; combining said gathered user data and said calculated key data to form said composed single data packet</u> ; transmitting said single data packet to the target storage device; determining whether said key data is valid; writing said user data into said target storage device only when said key data is valid.
3. The method of claim 1 further comprising: performing a boolean operation on selected bits of said user data to generate said key data.	2. The method of claim 1 further comprising: performing a boolean operation on selected bits of said user data to generate said key data.
4. The method of claim 1 further comprising: generating verification data from said user data at a controller of said target storage device; and comparing said key data in said single data packet with said verification data to determine if said key data matches said verification data.	3. The method of claim 1 further comprising: generating verification data from said user data at a controller of said target storage device; and comparing said key data in said single data packet with said verification data to determine if said key data matches said verification data.
5. The method of claim 4 further comprising: storing said user data to said target storage device if said key data matches said verification data.	4. The method of claim 3 further comprising: storing said user data to said target storage device if said key data matches said verification data.
6. The method of claim 1 further comprising: generating key data based on a destination address of said write operation.	5. The method of claim 1 further comprising: generating key data based on a destination address of said write operation.
7. The method of claim 1 further comprising: generating key data based on a system clock setting of said computer system.	6. The method of claim 1 further comprising: generating key data based on a system clock setting of said computer system.

8. A system for conducting a protected memory write to a storage device in a single transaction within a computer system, the system comprising: means for simultaneously delivering user data and key data to a controller of said storage device, wherein said user data is to be written to said storage device and said key data is used to establish authorization to store said user data; and means for determining whether said key data authorizes writing said user data to said storage device.	7. A system for conducting a protected memory write to a storage device in a single transaction within a computer system, the system comprising: means for simultaneously delivering user data and key data to a controller of said storage device, wherein said user data is to be written to said storage device and said key data is used to establish authorization to store said user data; and means, at an originating device, for calculating said key data using an algorithm before said user data and said key data is sent to said storage device; means for determining whether said key data authorizes writing said user data to said storage device; means for writing said user data to said storage device only when said key data authorizes writing said user data.
9. The system of claim 8 further comprising: means for writing said user data to said storage device only when said key data authorizes writing said user data.	7. A system for conducting a protected memory write to a storage device in a single transaction within a computer system, the system comprising: means for simultaneously delivering user data and key data to a controller of said storage device, wherein said user data is to be written to said storage device and said key data is used to establish authorization to store said user data; and means, at an originating device, for calculating said key data using an algorithm before said user data and said key data is sent to said storage device; means for determining whether said key data authorizes writing said user data to said storage device; <u>means for writing said user data to said storage device only when said key data authorizes writing said user data.</u>
10. The system of claim 8 further comprising: means, at an originating device, for calculating said key data using an algorithm before said user data and said key data is sent to said storage device.	8. The system of claim 7 wherein said algorithm calculates said key data from said user data.
11. The system of claim 10 wherein said algorithm calculates said key data from said user data.	8. The system of claim 7 wherein said algorithm calculates said key data from said user data.
12. The system of claim 8 wherein said determining means further comprises: means for generating verification data at said storage device controller; and means for comparing said verification data to said key data.	10. The system of claim 7 wherein said determining means further comprises: means for generating verification data at said storage device controller; and means for comparing said verification data to said key data.
13. The system of claim 8 wherein said determining means further comprises: means for authorizing writing of said user data only where said verification data matches said key data.	11. The system of claim 7 wherein said determining means further comprises: means for authorizing writing of said user data only where said verification data matches said key data.
14. The system of claim 11 wherein said algorithm calculates said key data based on a clock setting of said computer system.	9. The system of claim 8 wherein said algorithm calculates said key data based on a clock setting of said computer system.
15. A computer program product having a computer readable medium having computer program logic recorded thereon for protecting memory space in a target storage device during a write operation in a computer system, the computer program product	12. A computer program product having a computer readable medium having computer program logic recorded thereon for protecting memory space in a target storage device during a write operation in a computer system, the computer program product comprising: code for

comprising: code for composing a single data packet including user data and key data, wherein said user data is to be written to said target storage device and said key data is used to establish authorization to store said user data; code for transmitting said single data packet to said target storage device; and code for determining whether said key data is valid.	composing a single data packet including user data and key data, wherein said user data is to be written to said target storage device and said key data is used to establish authorization to store said user data, wherein the code for composing comprises: code for gathering user data for transmission to said target storage device; code for calculating key data based on said gathered user data; and code for combining said gathered user data and said calculated key data to form said composed single data packet; code for transmitting said single data packet to said target storage device; and code for determining whether said key data is valid.
16. The computer program product of claim 15 further comprising: code for writing said user data into said target storage device only when said key data is valid.	13. The computer program product of claim 12 further comprising: code for writing said user data into said target storage device only when said key data is valid.
17. The computer program product of claim 15 wherein the code for composing comprises: code for gathering user data for transmission to said target storage device; code for calculating key data based on said gathered user data; and code for combining said gathered user data and said calculated key data to form said composed single data packet.	15. The computer program product of claim 12 wherein the code for determining comprises: code for generating verification key data from said user data at a controller of said target storage device; and code for establishing said calculated key data as valid only if said generated verification key data matches said key data included in said single data packet.
18. The computer program product of claim 17 wherein the code for calculating comprises: code for performing a boolean operation on selected bits of said user data to generate said key data.	14. The computer program product of claim 12 wherein the code for calculating comprises: code for performing a boolean operation on selected bits of said user data to generate said key data.
19. The computer program product of claim 17 wherein the code for determining comprises: code for generating verification key data from said user data at a controller of said target storage device; and code for establishing said calculated key data as valid only if said generated verification key data matches said key data included in said single data packet.	15. The computer program product of claim 12 wherein the code for determining comprises: code for generating verification key data from said user data at a controller of said target storage device; and code for establishing said calculated key data as valid only if said generated verification key data matches said key data included in said single data packet.
20. The computer program product of claim 19 wherein said the code for generating verification data comprises: code for repeating said step of calculating key data at said controller of said target storage device.	16. The computer program product of claim 15 wherein the code for generating verification data comprises: code for repeating said step of calculating key data at said controller of said target storage device.

4. Claims 1-20 are rejected under the judicially created doctrine of anticipation-type double patenting as being anticipated by claims 1-13 of US Patent 6,473,844 (Farmer et al., "System and Method to Protect Vital Memory Space from Non-malicious Writes in a Multi Domain system"), as shown in the following table. Although not all of the

conflicting claims are exactly identical, they are extremely similar and are not patentably distinct from each other as shown below:

10/669,7845	6,473,844
1. A method for protecting memory space in a target storage device during a write operation in a computer system, the method comprising: creating a single data packet, including user data that is to be written to said target storage device and key data that is used to establish authorization to store said user data; transmitting said single data packet to the target storage device; determining whether said key data is valid; writing said user data into said target storage device only when said key data is, valid.	1. A method for protecting memory space in a target storage device during a write operation in a computer system, the method comprising the steps of: composing a single data packet including user data and key data, wherein the composing step includes: gathering user data for transmission to said data storage device, calculating key data based on said gathered user data, wherein the calculating step includes performing a boolean operation on selected bits of said user data to generate said key data, and combining said gathered user data and said calculated key data to form said composed single data packet; transmitting said single data packet to a data storage device; determining whether said key data is valid; and writing said user data into said data storage device only when said key data is valid.
2. The method of claim 1 further comprising: calculating key data based on said gathered user data; and combining said gathered user data and said calculated key data to form said composed single data packet.	1. A method for protecting memory space in a target storage device during a write operation in a computer system, the method comprising the steps of: <u>composing a single data packet including user data and key data</u> , wherein the composing step includes: gathering user data for transmission to said data storage device, calculating key data based on said gathered user data, wherein the calculating step includes performing a boolean operation on selected bits of said user data to generate said key data, and <u>combining said gathered user data and said calculated key data to form said composed single data packet</u> ; transmitting said single data packet to a data storage device; determining whether said key data is valid; and writing said user data into said data storage device only when said key data is valid.
3. The method of claim 1 further comprising: performing a boolean operation on selected bits of said user data to generate said key data.	1. A method for protecting memory space in a target storage device during a write operation in a computer system, the method comprising the steps of: composing a single data packet including user data and key data, wherein the composing step includes: gathering user data for transmission to said data storage device, calculating key data based on said gathered user data, wherein the calculating step includes <u>performing a boolean operation on selected bits of said user data to generate said key data</u> , and combining said gathered user data and said calculated key data to form said composed single data packet; transmitting said single data packet to a data storage device; determining whether said key data is valid; and writing said user data into said data storage device only when said key data is valid.
4. The method of claim 1 further comprising: generating verification data from said user data at a controller of said target storage device; and	2. The method of claim 1 wherein the determining step comprises the step of: generating verification key data from said user data at a controller of said data storage

comparing said key data in said single data packet with said verification data to determine if said key data matches said verification data.	device; and establishing said calculated key data as valid only if said generated verification key data matches said key data included in said single data packet.
5. The method of claim 4 further comprising: storing said user data to said target storage device if said key data matches said verification data.	1. A method for protecting memory space in a target storage device during a write operation in a computer system, the method comprising the steps of: composing a single data packet including user data and key data, wherein the composing step includes: gathering user data for transmission to said data storage device, calculating key data based on said gathered user data, wherein the calculating step includes performing a boolean operation on selected bits of said user data to generate said key data, and combining said gathered user data and said calculated key data to form said composed single data packet; transmitting said single data packet to a data storage device; determining whether said key data is valid; and <u>writing said user data into said data storage device only when said key data is valid.</u>
6. The method of claim 1 further comprising: generating key data based on a destination address of said write operation.	4. The method of claim 1 further comprising the step of: generating key data based on a destination address of said write operation.
7. The method of claim 1 further comprising: generating key data based on a system clock setting of said computer system.	5. The method of claim 1 further comprising the step of: generating key data based on a system clock setting of said computer system.
8. A system for conducting a protected memory write to a storage device in a single transaction within a computer system, the system comprising: means for simultaneously delivering user data and key data to a controller of said storage device, wherein said user data is to be written to said storage device and said key data is used to establish authorization to store said user data; and means for determining whether said key data authorizes writing said user data to said storage device.	6. A system for conducting a protected memory write to a storage device in a single transaction within a computer system, the system comprising: means for simultaneously delivering user data and key data to a controller of said storage device; and means for determining whether said key data authorizes writing said user data to said storage device; and an algorithm at a delivering device for calculating said key data, wherein said algorithm calculates said key data from said user data and based on a clock setting of said computer system.
9. The system of claim 8 further comprising: means for writing said user data to said storage device only when said key data authorizes writing said user data.	7. The system of claim 6 further comprising: means for writing said user data to said storage device only when said key data authorizes writing said user data.
10. The system of claim 8 further comprising: means, at an originating device, for calculating said key data using an algorithm before said user data and said key data is sent to said storage device.	6. A system for conducting a protected memory write to a storage device in a single transaction within a computer system, the system comprising: means for simultaneously delivering user data and key data to a controller of said storage device; and means for determining whether said key data authorizes writing said user data to said storage device; and <u>an algorithm at a delivering device for calculating said key data, wherein said algorithm calculates said key data from said user data and based on a clock setting of said computer system.</u>
11. The system of claim 10 wherein said algorithm calculates said key data from said user data.	6. A system for conducting a protected memory write to a storage device in a single transaction within a computer system, the system comprising: means for simultaneously delivering user data and key data to a controller of said storage device; and means for determining whether said

Art Unit: 2186

	key data authorizes writing said user data to said storage device; and <u>an algorithm at a delivering device for calculating said key data, wherein said algorithm calculates said key data from said user data and based on a clock setting of said computer system.</u>
12. The system of claim 8 wherein said determining means further comprises: means for generating verification data at said storage device controller; and means for comparing said verification data to said key data.	8. The system of claim 6 wherein said determining means further comprises: means for generating verification data at said storage device controller; and means for comparing said verification data to said key data.
13. The system of claim 8 wherein said determining means further comprises: means for authorizing writing of said user data only where said verification data matches said key data.	9. The system of claim 6 wherein said determining means further comprises: means for authorizing writing of said user data only where said verification data matches said key data.
14. The system of claim 11 wherein said algorithm calculates said key data based on a clock setting of said computer system.	6. A system for conducting a protected memory write to a storage device in a single transaction within a computer system, the system comprising: means for simultaneously delivering user data and key data to a controller of said storage device; and means for determining whether said key data authorizes writing said user data to said storage device; and an algorithm at a delivering device for calculating said key data, wherein said algorithm calculates said key data from said user data and <u>based on a clock setting of said computer system.</u>
15. A computer program product having a computer readable medium having computer program logic recorded thereon for protecting memory space in a target storage device during a write operation in a computer system, the computer program product comprising: code for composing a single data packet including user data and key data, wherein said user data is to be written to said target storage device and said key data is used to establish authorization to store said user data; code for transmitting said single data packet to said target storage device; and code for determining whether said key data is valid.	10. A computer program product having a computer readable medium having computer program logic recorded thereon for protecting memory space in a target storage device during a write operation in a computer system, the computer program product comprising: code for composing a single data packet including user data and key data, wherein the code for composing includes: code for gathering user data for transmission to said data storage device; code for calculating key data based on said gathered user data, wherein the code for calculating includes code for performing a boolean operation on selected bits of said user data to generate said key data; and code for combining said gathered user data and said calculated key data to form said composed single data packet; code for transmitting said single data packet to a data storage device; and code for determining whether said key data is valid.
16. The computer program product of claim 15 further comprising: code for writing said user data into said target storage device only when said key data is valid.	11. The computer program product of claim 10 further comprising: code for writing said user data into said data storage device only when said key data is valid.
17. The computer program product of claim 15 wherein the code for composing comprises: code for gathering user data for transmission to said target storage device; code for calculating key data based on said gathered user data; and code for combining said gathered user data and said calculated key data to form said composed single data packet.	12. The computer program product of claim 10 wherein the code for determining comprises: code for generating verification key data from said user data at a controller of said data storage device; and code for establishing said calculated key data as valid only if said generated verification key data matches said key data included in said single data packet.

Art Unit: 2186

<p>18. The computer program product of claim 17 wherein the code for calculating comprises: code for performing a boolean operation on selected bits of said user data to generate said key data.</p>	<p>10. A computer program product having a computer readable medium having computer program logic recorded thereon for protecting memory space in a target storage device during a write operation in a computer system, the computer program product comprising: code for composing a single data packet including user data and key data, wherein the code for composing includes: code for gathering user data for transmission to said data storage device; code for calculating key data based on said gathered user data, wherein the code for calculating includes code for <u>performing a boolean operation on selected bits of said user data to generate said key data</u>; and code for combining said gathered user data and said calculated key data to form said composed single data packet; code for transmitting said single data packet to a data storage device; and code for determining whether said key data is valid.</p>
<p>19. The computer program product of claim 17 wherein the code for determining comprises: code for generating verification key data from said user data at a controller of said target storage device; and code for establishing said calculated key data as valid only if said generated verification key data matches said key data included in said single data packet.</p>	<p>12. The computer program product of claim 10 wherein the code for determining comprises: code for generating verification key data from said user data at a controller of said data storage device; and code for establishing said calculated key data as valid only if said generated verification key data matches said key data included in said single data packet.</p>
<p>20. The computer program product of claim 19 wherein said the code for generating verification data comprises: code for repeating said step of calculating key data at said controller of said target storage device.</p>	<p>13. The computer program product of claim 12 wherein said the code for generating verification data comprises: code for repeating said step of calculating key data at said controller of said data storage device.</p>

5. ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Garcia et al. (US 6,151,689).

It is noted that, in the following claim analysis, those elements recited by the claims are presented using bold font.

As to claim 1, Garcia et al. discloses **a method for protecting memory space in a target storage device during a write operation in a computer system** [CPUs and I/O devices may write to, or read from, memory of a CPU of the system. Memory protection is provided by an access validation method maintained by each CPU in which CPUs and/or I/O devices are provided with a validation to read/write memory of that CPU, without which memory access is denied (abstract)], **the method comprising:**

creating a single data packet [figures 3A~3D and 4A~4C show various types of packets, comprising Header, Address, data and CRC], **including user data** [figures 3A~3D and 4A~4C show various types of packets, comprising Header, Address, data and CRC] **that is to be written to said target storage device** [figure 6, 24b is the target storage device] **and key data** [for example, the CRC may be the corresponding key data] **that is used to establish authorization to store said user data** [Use of CRC in this manner operates to protect message packets from end to end because the router elements do not modify or regenerate the CRC as the message packet passes through. The CRC of each message packet is checked at each router crossing. A command symbol--"This packet Good" (TPG) or "This Packet Bad" (TPB)--is appended to every packet (column 5, lines 39-45)];

transmitting said single data packet to the target storage device [see figure 6];

determining whether said key data is valid [If the received message packet is found to have a bad CRC (or it is tagged with a "This Packet Bad" (TPB) command symbol, see below) the packet is discarded, and access is denied (column 31, lines 22-25)]; **writing said user data into said target storage device only when said key data is valid** [CPUs and I/O devices may write to, or read from, memory of a CPU of the system. Memory protection is provided by an access validation method maintained by each CPU in which CPUs and/or I/O devices are provided with a validation to read/write memory of that CPU, without which memory access is denied (abstract)].

As to claim 2, Garcia et al. teaches that **the method of claim 1 further comprising:**
calculating key data based on said gathered user data [figures 3A~3D and 4A~4C show various types of packets, comprising Header, Address, Data and CRC, and CRC is calculated using Data]; **and**
combining said gathered user data and said calculated key data to form said composed single data packet [figures 3A~3D and 4A~4C show various types of packets, comprising Header, Address, Data and CRC].

As to claim 3, Garcia et al. teaches that **the method of claim 1 further comprising:**
performing a Boolean operation on selected bits of said user data to generate said key data [for example, the CRC may be the corresponding key data, which is calculated based on Boolean operations on Data bits].

As to claim 4, Garcia et al. teaches that **the method of claim 1 further comprising:**
generating verification data from said user data at a controller of said target storage device [Error-checking of the communication flow between the components of the processing system is achieved by adding a cyclic-redundancy-check (CRC) to the message packets that are sent between the elements of the system (column 5, lines 28-31)]; **and**
comparing said key data in said single data packet with said verification data to determine if said key data matches said verification data [The CRC of each message packet is checked not only at the destination of the message, but also while en route to the destination by each router element used to route the message packet from its source to the destination. If a message packet is found by a router element to have an incorrect CRC, the message packet is tagged as such, and reported to a maintenance diagnostic system (column 5, lines 31-40)].

As to claim 5, Garcia et al. teaches that **the method of claim 4 further comprising: storing said user data to said target storage device if said key data matches said verification data** [CPUs and I/O devices may write to, or read from, memory of a CPU of the system. Memory protection is provided by an access validation method maintained by each CPU in which CPUs and/or I/O devices are provided with a validation to read/write memory of that CPU, without which memory access is denied (abstract)].

As to claim 6, Garcia et al. teaches that **the method of claim 1 further comprising:**
generating key data based on a destination address of said write operation
[Accesses to the memory 28 are validated by 2) that the destination (e.g., CPU 12A) identified in the message packet is that of the receiver (column 31, lines 13-15)].

As to claim 7, Garcia et al. teaches that **the method of claim 1 further comprising:**
generating key data based on a system clock setting of said computer system
[FIG. 7B is an block diagram of a construction of the clock synchronization FIFO structure shown in FIG. 7A].

As to claim 8, refer to "As to claim 1."

As to claim 9, refer to "As to claim 5."

As to claim 10, refer to "As to claim 2."

As to claim 11, refer to "As to claim 2."

As to claim 12, refer to "As to claim 4."

As to claim 13, refer to "As to claim 5."

As to claim 14, refer to "As to claim 7."

As to claim 15, refer to "As to claim 1."

As to claim 16, refer to "As to claim 5."

As to claim 17, refer to "As to claim 2."

As to claim 18, refer to "As to claim 3."

As to claim 19, refer to "As to claim 4."

As to claim 20, refer to "As to claim 4." Also see figure 6 of Garcia et al.

Conclusion


7. Claims 1-20 are rejected as explained above.
8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sheng-Jen Tsai whose telephone number is 571-272-4244. The examiner can normally be reached on 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Matthew Kim can be reached on 571-272-4182. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Sheng-Jen Tsai
Examiner
Art Unit 2186

December 21, 2006


MATTHEW KIM
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100